Report on the Maturity of the Library's System Development Life Cycle Processes and Procedures
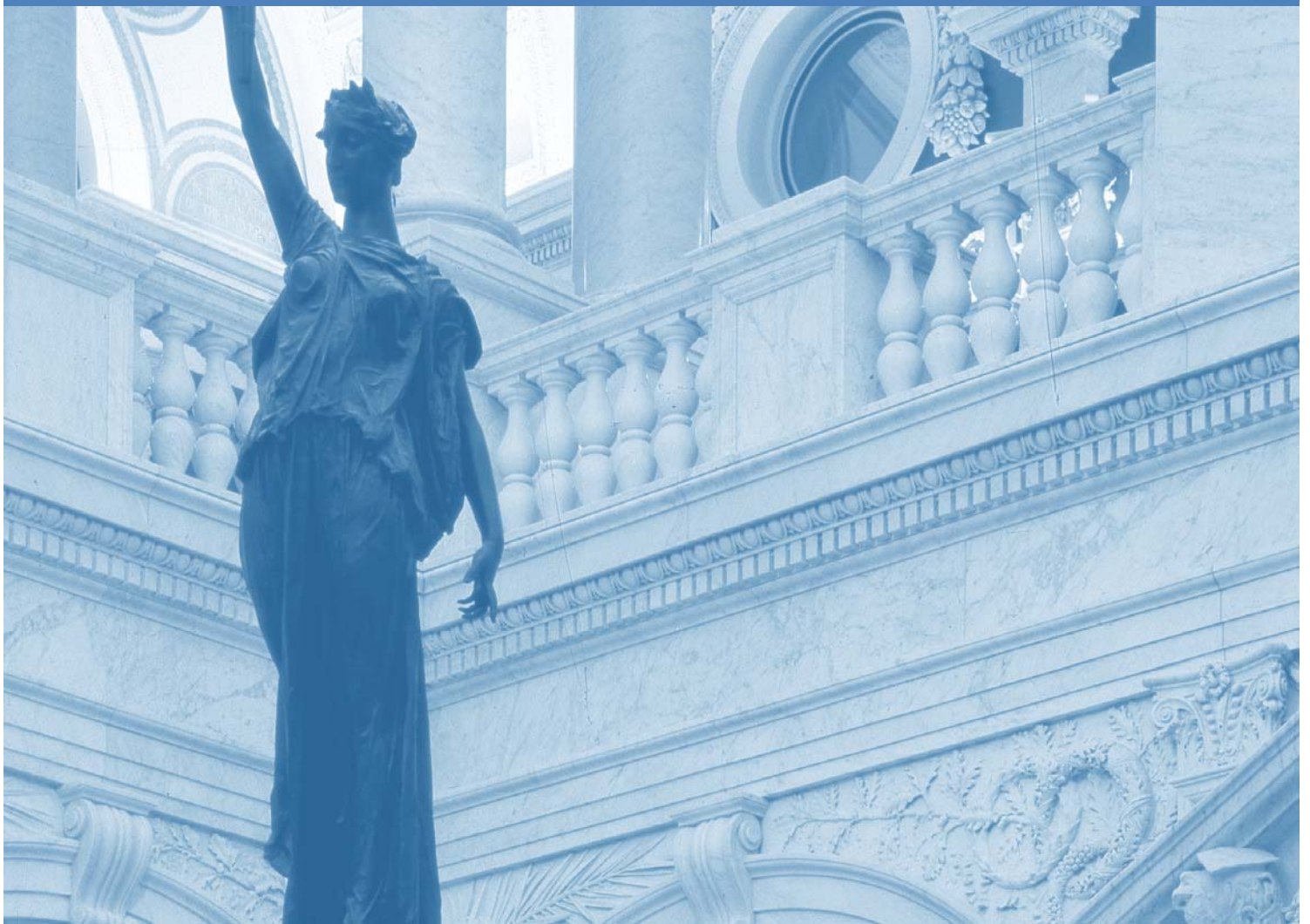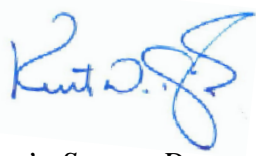
Library of Congress Office of the Inspector General

OFFICE OF THE INSPECTOR GENERAL

LIBRARY OF CONGRESS

101 INDEPENDENCE AVE
WASHINGTON, D.C. 20540

February 25, 2015

MEMORANDUM FOR: James H. Billington
                                 Librarian of Congress

FROM: Kurt W. Hyde
                                 Inspector General

SUBJECT: *Maturity of the Library's System Development Life Cycle Processes and Procedures*
                                 Report No. 2013-IT-105

This transmits the audit report summarizing the results of CliftonLarsonAllen's (CLA's) audit of the Library's System Development Life Cycle processes and procedures. The Executive Summary begins on page *i*, and the full text of CLA's findings and recommendations appear in Appendix A.

Based on management's written response to the draft report, we consider all of the recommendations resolved except for recommendation 2. Please provide, within 30 calendar days, an action plan addressing implementation of the resolved recommendations, including an implementation date, in accordance with LCR 2023-9, *Rights and Responsibilities of Library Employees to the Inspector General*, §6.A. For recommendation 2, please provide a date for completing your assessment of the recommendation along with related action plan(s).

We appreciate the cooperation and courtesies extended by Information Technology Services during this audit.

cc: Deputy Librarian of Congress
     Chief of Staff
     Interim Chief Information Officer

Summary

The System Development Life Cycle (SDLC) process applies to information system development projects ensuring that all functional and user requirements are met by using a structured and standardized process during all phases of a system's life cycle. Systems developed according to information technology (IT) best practices are more likely to provide secure and reliable long-term performance.

The Office of the Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to perform an audit of the Library's SDLC process to assess the maturity of the Library's current policies and practices and to evaluate the efficiency of Information Technology Services' (ITS) process for structuring, planning, and controlling the development of the Library's vital information systems. This included an assessment of ITS' compliance with the Library's SDLC policy and the application of generally accepted IT best practices.[1]

In its report,[2] CLA identified several weaknesses in the Library's SDLC process that places the Library at risk of developing IT systems that are not adequately documented and lack cost and performance data needed to properly monitor and make prudent IT investment decisions. By optimizing its current SDLC process, the Library can mitigate these risks while improving efficiency and governance of IT system development.

In addition, CLA found the following weaknesses in the Library's SDLC governance structure:

ITS Information Technology Project Management Is Not Applied Library-Wide—Library management of its IT projects was ineffective due to a decentralized Project Management Office (PMO) and SDLC methodology. As a result, each service unit within the Library uses different approaches to manage IT projects.

CLA recommends that the Office of the Librarian issue a Library-wide policy for the system development life cycle process. CLA also recommended establishing a Library-wide PMO to communicate and enforce the Library's Project Management Life Cycle/SDLC methodology and to ensure the Library's major IT projects are effectively managed in a consistent manner across all service units. CLA also recommends that the Office of the Librarian centralize the assessment of the Library's IT portfolio with the PMO and prohibit the existing practice of service unit IT investment self-assessments.

The Library has not established a Repeatable Process for Internal or External Evaluations of its IT Projects and no Central Data Repository was Maintained—The Library's Enterprise Architect (EA) has not performed (and does not have the mandate to perform) a comprehensive evaluation of the Library's IT projects. As a result, the EA's repository is not considered a reliable central data

---

[1] CLA evaluated the Library's SDLC processes using the Government Accountability Office's (GAO) *Federal Information System Control Audit Manual*, ISO/IEC 12207 *System and software engineering – Software life cycle processes*, SEI *CMMI for Development, Version 1.3*, and GAO's *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (March 2004).

[2] CLA is responsible for the conclusions expressed in the attached report dated February 17, 2015. We performed limited oversight of CLA's work including defining deliverables in the contract's statement of work, reviewing CLA's audit plan, attending the entrance and exit conferences, and conducting regular engagement status meetings. We also facilitated communications between ITS management and CLA.

repository that service units can use for their internal reviews and oversight of their IT projects. CLA recommends that the Office of the Librarian establish a central data repository with the EA and/or PMO to store all project artifacts, including cumulative cost and schedule data. In addition, periodically perform an internal and/or external inspection of the Library's IT projects and update the EA repository with the results of the inspection if necessary.

No Cumulative Cost and Schedule Documentation—ITS did not maintain cumulative cost and schedule data as this was separately managed by each service unit with the assistance of ITS managers. As a result, management's ability to monitor programs and projects effectively is negatively impacted.

CLA recommends that the Office of the Librarian establish a budget methodology to track project development costs and measure variances against approved costs. CLA also recommended revising Library of Congress Regulation 1600[3] to clearly delineate ownership and stewardship of IT assets.

No ITS/PMO Oversight; Ineffective Monitoring of Library IT Projects— The ITS Project Management Life Cycle guide was not effectively communicated or consistently applied throughout the Library which resulted in inconsistent management, a lack of accountability, and ineffective stewardship over the Library's major IT projects.

CLA recommends that the Office of the Librarian issue a Library-wide policy that communicates the mandatory requirements of the Library's SDLC process outlined in the existing ITS Project

Management Guide to ensure consistent management of the Library's IT projects.

Significant Life Cycle Milestone Deliverables for Certain Systems Were Not Documented or Executed— CLA found that Library Service's System Management Information Network II went through an exhaustive system modernization and received an authorization to operate without oversight and approval from the IT Steering Committee (ITSC) even though the project met three of the threshold criteria for ITSC oversight. In addition, CLA found that one other project reviewed in Library Services had incomplete or missing system development documentation.

CLA recommends disciplined performance and quality reviews (preferably by the PMO) on all major SDLC projects.

Management agreed with all recommendations except to establish a centralized Library-wide PMO. Although management agreed that central oversight of IT projects is valuable, it did not agree that establishing a separate PMO was the most efficient approach. Instead, management stated they would assess whether to assign this function to the ITSC (or another existing body) or establish a new office. OIG believes that a central PMO can communicate and enforce the Library's Project Management Life Cycle /SDLC methodology better and ensure IT projects are effectively managed.

---

[3] *Information Resource Management Policy and Responsibilities*, October 2012.

Table of Contents

Appendix A: CLA Report/Management's Response

LIBRARY OF CONGRESS

**REPORT ON THE MATURITY OF THE LIBRARY'S SYSTEM DEVELOPMENT
LIFE CYCLE PROCESSES AND PROCEDURES**

AS OF JUNE 30, 2014

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

February 17, 2015

Mr. Kurt W. Hyde
Inspector General
U.S. Library of Congress
101 Independence Avenue, SE, Room No. LM-630
Washington, DC 20540

Dear Mr. Hyde:

CliftonLarsonAllen LLP is pleased to submit its report on the Library of Congress Information Technology System Development Life Cycle (SDLC) Processes and Procedures. The purpose of this review was to assess the maturity of current policies and practices and to evaluate the efficiency of Information Technology Services' (ITS) process for structuring, planning and controlling the development of the Library's vital information systems. This included an assessment of ITS' compliance with the Library's SDLC policy and the application of generally accepted IT Best Practices.

We conducted our audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States (also known as generally accepted government auditing standards).

Our audit methodology also adhered to the policies and procedures specified in the U.S. Government Accountability Office (GAO)/President's Council on Integrity and Efficiency and GAO's Federal Information System Controls Audit Manual, as amended and cross-referenced to standards issued by the International Organization for Standardization, the Software Engineering Institute's Capability Maturity Model Integration Standards, and other applicable government standards and guidance.

Our testing was based on our independent evaluation of the policies and practices in place as of June 30, 2014. In preparing our report, we collaborated with LOC management at the different Service Units and value their cooperation in this effort. We appreciate the opportunity to assist your office with this report. Should you have any questions, please call me at (301) 931-2050.

Very truly yours,

CLIFTONLARSONALLEN LLP

CliftonLarsonAllen LLP

LIBRARY OF CONGRESS
SYSTEM DEVELOPMENT LIFE CYCLE EVALUATION

TABLE OF CONTENTS

LIBRARY OF CONGRESS
SYSTEM DEVELOPMENT LIFE CYCLE EVALUATION

I. EXECUTIVE SUMMARY

The Information Technology Services (ITS) of the Office of Strategic Initiatives (OSI) is centrally involved in the acquisition, design, implementation and maintenance of information systems which are vital to the Library of Congress' (LOC or Library) mission. In this capacity, they strive to comply with the Software Engineering Institute's (SEI) Capability Maturity Model Integration (CMMI) and other industry-recognized standards in their system development methodology. Systems developed according to generally accepted information technology (IT) standards will most likely provide secure and reliable long term performance.

The Office of the Inspector General (OIG) contracted CliftonLarsonAllen LLP (CLA, we or our) to evaluate the operating effectiveness of the Library's current System Development Life Cycle (SDLC) methodology by reviewing, analyzing, and assessing the maturity level of these processes using standards set out by the International Organization of Standardization (ISO) and the SEI's Maturity Model and determining whether the Library is compliant with those standards.

We used the CMMI maturity scorecard[1] to evaluate a sample of projects that we selected for testing. Our sample consisted of all IT related projects involving mission-critical systems (major IT projects) that were initiated or completed on or after January 1, 2011 (after the implementation of the Information Technology Steering Committee (ITSC)). IT Systems are considered Major IT Systems, when they require special management attention because of their importance to the mission or function of the agency. Acquisitions with high development, operating or maintenance costs, or high visibility are also considered major IT systems.

Based on a CMMI maturity scale of 1 – 5 (where 1 denotes LOC management selected projects in an unstructured, ad hoc manner, project outcomes were unpredictable and successes were not repeatable and 5 denotes good processes were followed and automated), LOC's maturity can be rated between 2 and 3, where 2 is *Managed* (processes are characterized but are often reactive) and 3 is *Defined* (projects reviewed were tailored in conformity with LOC standards and SDLC Best Practice). The reason for this disparity is the inconsistent manner in which projects were executed among the different Service Units (SUs), with some SUs maintaining better documentation than others.

A graphical representation of LOC's SDLC maturity model is portrayed in figure 1 below:

---

[1] *The Capability Maturity Model Integration (CMMI) scorecard is an assessment methodology that rates an entity's process maturity on a scale from 1 – 5 with 1 being processes are unstructured or ad-hoc to 5 where processes are optimized.*

LIBRARY OF CONGRESS
SYSTEM DEVELOPMENT LIFE CYCLE EVALUATION

LOC'S System Development Life Cycle Maturity Model					
Non Existent	**Initial/ Ad Hoc**	**Repeatable but Reactive**	**Defined Process**	**Managed and Measurable**	**Optimized**
0	**1**	**2**	**3**	**4**	**5**

Legend For Symbols Used

LOC's Current Maturity Level

Industry standard

Legend For CMMI Maturity Ranking

0. Management Processes are nonexistent or not applied.

1. Processes are ad hoc and Reactive

2. Processes follow a regular pattern

3. Processes are documented and Communicated

4. Processes are monitored and measured
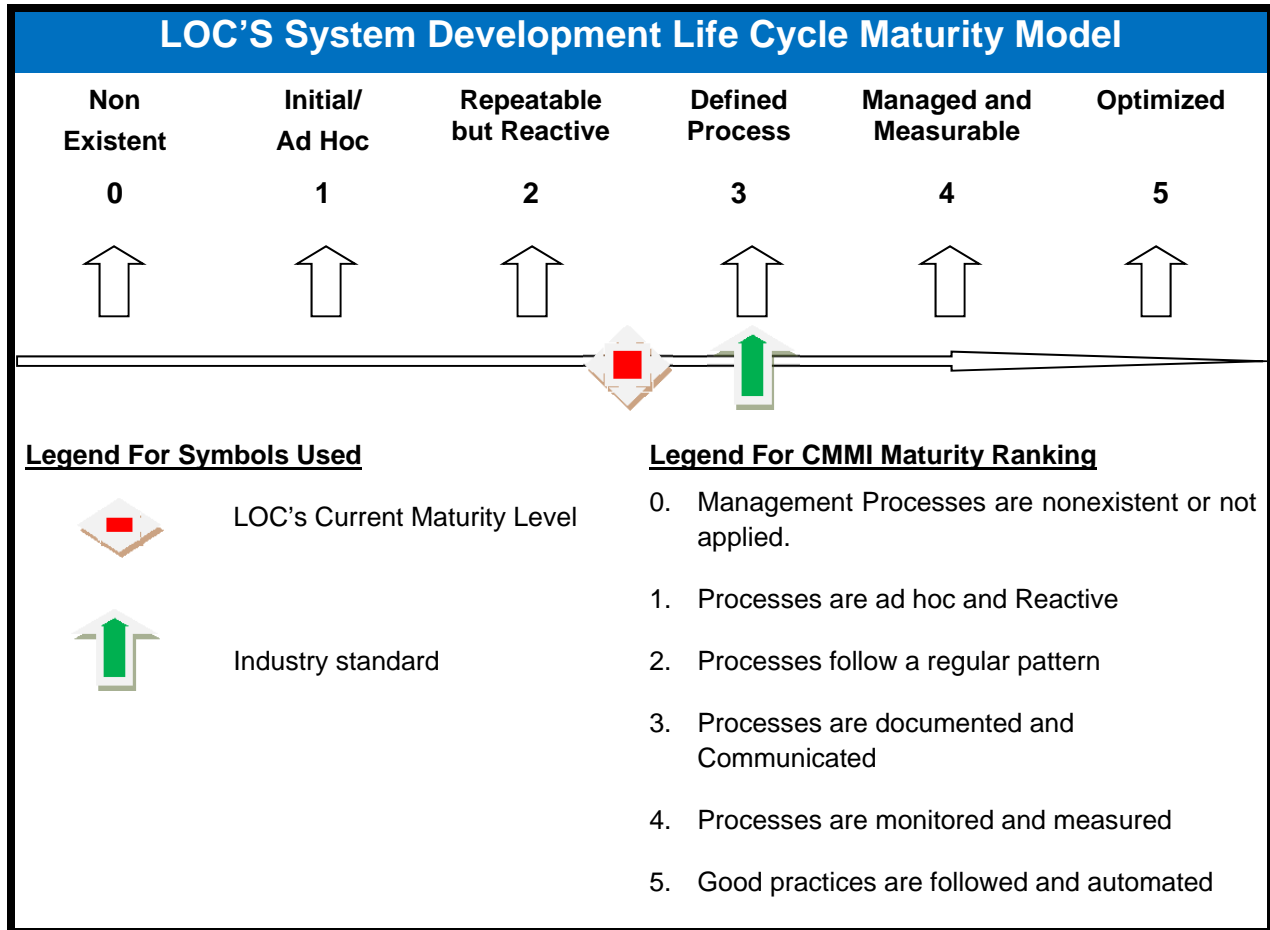
5. Good practices are followed and automated

Figure 1: LOC Maturity table

LOC has had long standing deficiencies with information technology due to a lack of standardization of its processes, coupled with a lack of fiscal discipline[2]. These deficiencies, initially seen as a result of a decentralized IT management environment, have prompted management to set as one of its Strategic Goals[3] "*to improve information technology governance and investment processes*".

The "*Outcomes and Results Statement*" of the 2011-2016 Strategic Plan indicates that the Library's infrastructure optimally supports accomplishment of the Library's strategic goals:

> "…The Library's enterprise architecture [EA] is the authoritative operational and technical frame-of-reference that ensures proposed technology solutions meet identified business needs, thereby improving mission performance and accountability…"

Our review of the Library's SDLC methodology found the following weaknesses:

---

[2] *See conclusions documented in the Report on the Library's Certification and Accreditation Policies, Procedures and Operating Effectiveness (October 2014).*
[3] *See Library of Congress – Strategic Plan – Fiscal Years 2011 – 2016.*

LIBRARY OF CONGRESS
SYSTEM DEVELOPMENT LIFE CYCLE EVALUATION

1. LOC's management of its IT projects was ineffective due to the absence of a Library-wide SDLC process. The Library also lacks accounting for asset development/implementation costs (i.e. accounting for and capitalizing labor costs incurred by personnel in the development, testing and implementation of information systems). Although the ITS' Project Management Office (PMO) has provided adequate guidance by way of an SDLC Plan developed in 2006 which covers all the steps required by industry best practice for a well-designed SDLC process, these resources are not considered overarching Library policy and ITS has no mandate to enforce such guidance.

2. Certain systems were missing key milestone deliverables (management checkpoints) in their development life cycle. Missing documentation included project charters, evidence of ITSC oversight and approval (for projects that meet the ITSC threshold), evidence of technical and user test approval documentation, and implementation plans/timetables.

   These conditions occurred because the Library did not fully centralize its IT investment management functions as they relate to the SDLC process. The Library needs to have one centralized PMO to communicate and enforce the Library's Project Management Life Cycle (PMLC)/SDLC methodology and to ensure LOC's IT projects are effectively managed. ITS has assigned Research and Development (R&D) managers to assist each Service Unit (SU) in managing its IT projects but the R&D managers do not handle all projects included in each SU's portfolio; consequently, some projects under the direct management of the SUs may not be managed in line with the ITS process. We could not determine the value of these projects managed outside of direct ITS oversight as this information could not be readily provided leaving some amount of LOC's IT projects at risk.

   This lack of a centralized or Library-wide process increases the risk that IT investments could experience cost and schedule overruns, which could ultimately lead to other costly, unproductive, or failed programs and projects.

We recommend that the Office of the Librarian:

- Issue a Library-wide policy that communicates the mandatory requirements of the SDLC process outlined in the existing ITS Project Management Guide to ensure consistent management of LOC's IT projects.

- Establish a centralized Library-wide PMO that would implement policies, procedures, and controls to guarantee uniform management of LOC's IT investment portfolio. These actions are needed to reduce the risk of loss while improving management control and corporate governance of major IT investments.

- Conduct performance and quality reviews on all major programs and projects in LOC's IT investment portfolio.

- Empower the PMO with a mandate to implement controls to continuously monitor all programs and projects in LOC's IT investment portfolio.

- Establish a central data repository with the Enterprise Architect and/or PMO to store all project artifacts, including cumulative cost and schedule data. In addition, perform reoccurring inspections to ensure its accuracy.

- Centralize IT investment assessments with the PMO and prohibit SU self assessments.
- Revise LCR 1600 to clearly delineate ownership and stewardship of IT assets

II. BACKGROUND AND BUSINESS PROFILE

As an agency of the legislative branch, the LOC includes seven internal divisions (or Service Units), including the Office of the Librarian, Congressional Research Service, U.S. Copyright Office, Law Library, Library Services, the OSI and the Office of Support Operations. The OIG oversees all Library programs and operations and has the independence to decide which activities to review. It conducts audits, investigations and other reviews and reports semi-annually to the U.S. Congress.

The Library relies on its IT systems and information to achieve its mission. Protecting IT systems and information is a shared responsibility between SUs and ITS, a directorate located in the OSI program service unit.

The mission of the LOC is to support the Congress in fulfilling its constitutional duties and to further the progress of knowledge and creativity for the benefit of the American people. LOC's strategic goals are to:

- Provide authoritative research, analysis, and information to the Congress.
- Acquire, preserve, and provide access to a universal collection of knowledge and the record of America's creativity.
- Sustain an effective national copyright system.
- Lead and work collaboratively with external communities to advance knowledge and creativity.
- Manage proactively for demonstrable results.

Library of Congress Regulation (LCR) 1600 establishes uniform policy and responsibilities for Information Resource Management (IRM) in the Library. It provides the foundation for an overall approach to IRM throughout the Library whereby IRM is integrated with the Library's strategic plan and reinforces the Library's Management Agenda. The regulation addresses the key concepts that support IRM, EA, and Information Technology Investment Management (ITIM).

Per LCR 1600 Section 5 (a), "The Librarian is responsible generally for oversight of the Library's IRM plan and for all final determinations regarding the Library's IRM policy and IT investments." Section 5 (b) states the Executive Committee (EC) is responsible for appointing individuals to the ITSC and Architecture Review Board (ARB), providing strategic mission and priority guidance to the ITSC, monitoring and directing appropriate actions on results of key efforts and executive-level reports and recommendations for ITIM processes, and reviewing Congressional Budget request recommendations for Library IT investments.

R&D managers conduct Project Management Reviews, milestone reviews, and operational analysis. Moreover, OSI/PMO develops IT project management policies and procedures.

On March 24, 2010, the ITSC charter was created to support IRM and IT governance throughout the Library. According to the charter, the ITSC takes direction from and reports to the Executive Committee. The ITSC provides input, advice and direction to the ARB that reports to it.

ITS SDLC Project Management

Within OSI, the PMO is responsible for monitoring and reporting on resource, schedule, scope and overall performance goals and variances for all ITS projects. This includes IT initiatives that meet the IT Steering Committee thresholds, initiatives for which the PMO has been notified by the SU, and all ITS sponsored projects. Accordingly, PMO conducts milestone reviews (for projects that it supervises), which provide a basis for comprehensive management, progressive decision-making, and authorization of funding for each phase of the SDLC framework. By monitoring and measuring progress on a regular basis at each milestone, project managers should be able to identify variances and take appropriate corrective action.

III.   OBJECTIVE

CLA was contracted by the LOC OIG to evaluate the maturity of the Library's SDLC process as an integral part of the task order issued for the Legislative Branch Agencies serviced by the Library of Congress' Financial Statement Audit Contract (LCOIG11C0005).

The audit objectives were to determine whether ITS's SDLC policies and procedures adequately address Federal requirements and IT best practices governing the SDLC process and to determine the effectiveness of the ITS implementation of this SDLC process.

IV.   SCOPE AND METHODOLOGY

CLA performed this evaluation of ITS's SDLC methodology from May through July 2014 in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States (also known as generally accepted government auditing standards). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit also adhered to the specific policies and procedures as specified in the Government Accountability Offices' Federal Information System Controls Audit Manual (GAO/FISCAM), as amended and cross-referenced to standards issued by the ISO, the SEI's[4] CMMI for Development Version 1.3 Standards, and other applicable government standards and guidance.

SCOPE

We analyzed a stratified sample of IT projects including IT systems that are under the oversight of the ITSC and those that are not. This stratified sample, including systems from all SUs, was divided into two distinct strata based on the relative size of the IT project (medium to large scale projects). The universe included LOC's new projects and ongoing projects designated as having significant IT enhancements and/or upgrades between FY 2011 and FY 2014[5].

In October 2010, the Library adopted a new threshold policy for determining IT projects that must go through the ITSC for vetting/approval as follows:

---

[4] *Carnegie Mellon University's Technology Commercialization Enterprise*
[5] *The review date covers the period immediately following the implementation of the ITSC Charter to test operating effectiveness of procedures after inception of the charter.*

LIBRARY OF CONGRESS
SYSTEM DEVELOPMENT LIFE CYCLE EVALUATION

    a. All IT projects that impact another service, infrastructure or department,
    b. Estimated three year cost of acquisition development, operation and maintenance is equal to or greater than $1,000,000,
    c. Software enhancements are significant or require complex implementation,
    d. The project is high risk,
    e. The effort has high visibility internally or externally, or
    f. The investment provides new common technology infrastructure.

We determined whether ITS's SDLC process was adequate and comparable to Federal standards and IT best practices by comparing them to the ISO standards. We also evaluated the effectiveness of ITS' management of LOC's IT projects. We reviewed 39 "Mission Critical" applications and general support systems. Of the 39 systems, we selected 15 ongoing or completed projects, which included 12 new projects and 3 projects in the process of decommissioning. (This sample size represented 100% of projects that underwent significant changes during the period under review). These 15 projects and their sub-component projects were in various phases of the life cycle process. (See Table 1 for the IT projects reviewed and a description of each).

#	Service Unit	System	New Implementation/ Upgrade	De-Commissioned Systems	Compliant with ITS SDLC Methodology (Y/N)
1.	Copyright Office	Electronic Copyright Office (eCO)	X		Y
2.	Copyright Office	Copyright Imaging System (CIS)		X	Y
3.	Law Library/ Congressional Research Service	Thomas		X	Y
4.	Congressional Research Service	CRS.gov Client and Web Services	X		Y
5.	Congressional Research Service	Inquiry Status & Information System (ISIS) – *Replaced by Mercury Request Management System (RMS)*		X	Y
6.	Congressional Research Service	Mercury Request Management System (RMS)	X		Y
7.	Congressional Research Service	Beta.Congress.Gov	X		Y
8.	Office of the Librarian	Momentum Financial System	X		Y
9.	Office of the Librarian	Correspondence Control Management	X		Y

#	Service Unit	System	New Implementation/ Upgrade	De-Commissioned Systems	Compliant with ITS SDLC Methodology (Y/N)
		System (ccmMercury)			
10.	Office of the Librarian	LC Budget System(LCBS) (Clarity)	X		Y
11.	Office of the Librarian	Financial Reporting System (FRS)	X		Y
12.	Office of Support Operations (HR)	Web Time & Attendance (WebTA)	X		Y
13.	Library Services	Voyager - Integrated Library System (ILS)	X		N
14.	Library Services	Federal Library & Information Network (FEDLINK) Customer Accounting Management System (FCAMS)	X		Y
15.	Library Services	System Management Information Network II (SYMIN II)	X		N
TOTAL			12	3	

Table 1 – Sampled IT Projects

METHODOLOGY

Our review of major IT projects focused on the assessment of final versions of project documentation, corresponding to the most recently completed milestone review. We developed a list of the required documents for each milestone using the PMLC/SDLC phased approach (see figure 2) and ISO 12207 maturity model. We assessed all of the available documents required for a project to progress from one milestone to the next in the SDLC process, including the concept of operations, project charter, project management plan, risk management plan, and the acquisition management plan (for Commercial Off the Shelf (COTS) products), amongst others. We considered all SDLC documents equally critical to the process. Finally, we conducted interviews with the PMO and ITS senior management, system owners and R&D managers to determine their roles and responsibilities in the SDLC process.

Using the CMMI maturity scorecard, we evaluated the projects selected for testing. Our sample consisted of all projects involving mission-critical systems that were initiated or completed on or after January 1, 2011 (after the implementation of the ITSC). Our scorecard was based on the following maturity levels, where 0 denotes procedures are nonexistent, and 5 represents a fully optimized process.

Maturity Level	Description
Level 0	*Non-Existent:* Management Processes are non-existent or not followed at all
Level 1	*Initial*: Processes are unpredictable, poorly controlled and reactive.
Level 2	*Managed*: Processes are characterized for projects but are often reactive.
Level 3	*Defined*: Projects tailor their processes from Management's Standards.
Level 4	*Quantitatively Managed*: Processes are measured and controlled.
Level 5	*Optimized*: Management focus on Process Improvement.

Table 2 – Maturity Levels Description

At level 1 maturity, an agency is selecting projects in an unstructured, ad hoc manner. Project outcomes are unpredictable and successes are not repeatable. At stage 3, the agency is creating awareness of the investment process, while the most advanced organizations, operating at Stage 5 maturity, benchmark their IT investment processes relative to other "best-in-class" organizations and look for breakthrough information technologies that will enable them to change and improve their business performance.

ITS uses a seven-phased approach to manage information technology-related projects throughout their life cycle. These phases are depicted in the following diagram. A brief description of each phase is provided below:

SDLC Phases

1. Requirements & Analysis
2. Design
3. Development
4. Test
5. Implementation
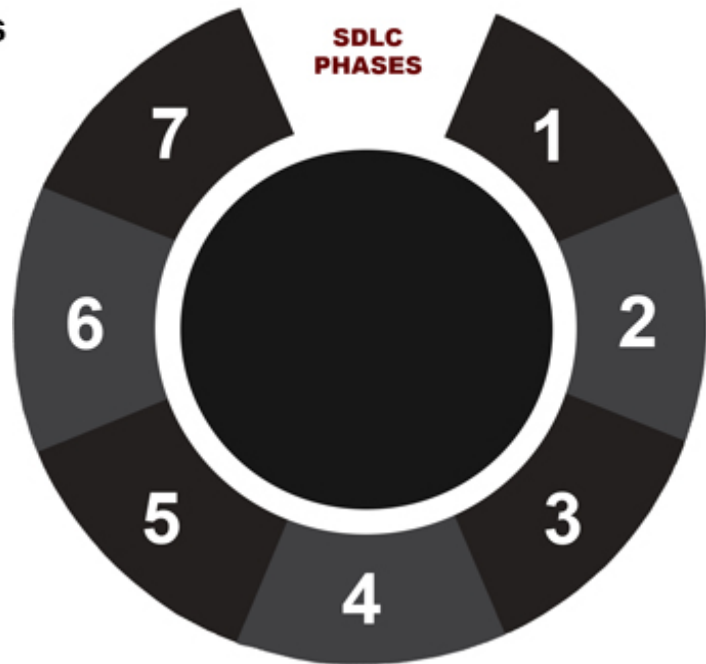6. Operations
7. Disposition

Figure 2: ITS SDLC Phases

Phase 1: Requirements and Analysis: The Planning & Requirement Analysis (P&RA) Phase begins with reviewing the composition of the Project Team and making any adjustments that are needed; this is followed with establishing relationships with stakeholders. In some situations, the decision is made to complete a Concept of Operations (CONOPS) document prior to the Requirement Document (RD).

Phase 2: Design: Transforms detailed requirements definitions into complete, detailed system specifications. It focuses on how the system will deliver the required functionalities that were ascertained in the P&RA phase. A blueprint is created that satisfies all documented requirements, whether the system is developed in-house or purchased as a COTS product. It is important to note that purchasing a COTS product does not absolve the team from having to perform design, some degree of development and integration.

Phase 3: System Development: The design is converted into a complete information technology system. During the development phase the software product is designed, created and tested and will result in a software product ready to be released to the customer. The choice of developing method often depends on the present situation.

Phase 4: Testing: Validates whether the developed system meets the system requirements and is ready to be deployed. Three types of tests are envisaged: (1) System Qualification Test (SQT); (2) Security Test and Evaluation (ST&E); and (3) System Acceptance Test (SAT) commonly called User Acceptance Test (UAT).

Phase 5: Implementation: The tested configuration is brought live for operational use in the Production Environment. The system can either be a pilot or migrated straight into production depending on the development methodology employed on the project.

Phase 6: Operations: This phase describes tasks for maintenance and operation of systems in a production environment. The operation and maintenance phases occur simultaneously, the operation-phase consists of activities such as assisting users in working with the created software product, while the maintenance-phase consists of maintenance-tasks to keep the product up and running. The maintenance includes any general enhancements, changes and additions, which might be required by the end-users. These defects and deficiencies are usually documented by the developing organization to enable future solutions and known issues addressed in any future maintenance releases.

Phase 7: Disposition: This phase describes end-of-system activities. Emphasis is given here to proper preservation of data and disposing of the system in a responsible manner. It is important that data, procedures and documentation are packaged and archived in an orderly fashion and in accordance with LOC policies regarding retention of electronic records.

ITS's SDLC process is outlined in the Library's Intranet (www.loc.gov/staff/pmo/sdlc.html).

V. DETAILS OF RESULTS

The Library Has Not Adequately Implemented Management Controls to Ensure Library-Wide Governance of LOC's IT Projects

Effective governance enables an organization to manage its projects in a disciplined and consistent manner so they have an improved chance of being completed on time and within budget. Capital investment policies support project management principles by guiding Federal agencies in the selection and management of IT projects and by ensuring that IT resources are used efficiently and are aligned with the agency's mission. LCR 1600 established ITIM, the ARB and the ITSC, to ensure a structured approach to system development and to provide systematic checks and balances annually at critical points in the project life cycle.

CLA evaluated the Library's processes against GAO's *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (March 2004). This framework is built around the "select/control/evaluate" approach described in the Clinger-Cohen Act of 1996, which establishes statutory requirements for IT management. The framework provides a method for evaluating and assessing how well an agency is selecting and managing its IT resources. Using the framework to analyze an agency's IT investment management processes provides: (1) a rigorous, standardized tool for internal and external evaluations of these processes; (2) a consistent and understandable mechanism for reporting the results of assessments; and (3) a road map that agencies can follow in improving their processes.

While the Library is not subject to Executive Branch Directives, the GAO framework lays a good foundation used by many federal agencies in analyzing their investment management process or in determining the maturity of its investment process.

We noted weakness in LOC's SDLC governance structure as follows:

1. **ITS Information Technology Project Management Is Not Applied Library-Wide**.

    LOC's management of its IT projects was ineffective due to a decentralized PMO and SDLC methodology. As a result, each SU within LOC uses different approaches to manage IT projects. While initial projects costs are captured for the most part, LOC does not have a process for accounting for asset development/implementation costs (accounting for and capitalizing labor costs utilized by LOC personnel in the development, testing and implementation of information system enhancements). [These deficiencies were reported in CLA's audit of the Certification and Accreditation process, where it was noted that the Library could not ascertain capitalizable IT (software) implementation costs due to the fact that management did not adequately capture internal personnel costs related to product development]. Although the ITS' PMO has provided adequate guidance by way of an SDLC Plan developed in 2006 coupled with an Intranet website[6], these resources are not considered overarching Library policy and ITS has no mandate to enforce such guidance.

    This decentralized IT management style violates LCR 1600 Section 5 (A) which designates the Librarian as the oversight authority over the Library's IRM and grants him the responsibility for all final determinations regarding IT projects. This lack of a

---

[6] *The website is complete but is currently undergoing enhancements such as populating the SDLC flowcharts with process narratives.*

centralized process increases the risks that IT projects could experience cost and schedule overruns, which could ultimately lead to other costly, unproductive, or failed programs and projects.

The SDLC steps and flowcharts outlined in the ITS/PMO intranet are adequate and comparable to Federal standards and IT best practices. However, ITS did not have the mandate to communicate or enforce mandatory requirements outlined in the guide but relies on its R&D managers to enforce these guidelines as they supervise the projects at the different SUs that they support. Given that the current directive shares the stewardship responsibility over LOC's IT projects between "ITS and IT staff within service units", it is vital that immediate action is taken to implement management controls to ensure centralized oversight of LOC's IT projects.

2. **LOC has not established a Repeatable Process for Internal or External Evaluations of its IT Projects and no Central Data Repository was Maintained**

The Enterprise Architect in OSI has not performed (and does not have the mandate to perform) a comprehensive evaluation of the Library's IT projects. The EA maintains a working repository (Enterprise Architecture Collaborative Workspace Database) to store metadata about the Library's IT systems. However, this repository has not been updated for over two years. The content of this repository was unreliable as the sources of data were never validated by the subject matter experts or program managers with adequate knowledge of the systems within each SU. Data in the repository was not entered from an exhaustive internal/external evaluation but rather from informal interviews with different personnel at the different SUs.

During our review of certain Library Services (LS) projects, we requested access to the project documentation for sampled projects. We were directed to as many as four different file locations to retrieve project documentation and were unable to obtain all the project milestone documentation related to one project (out of three projects reviewed within LS).

Documentation for each project is reviewed by SU's change control boards and required at the completion of a milestone when the milestone review briefing is conducted. Enforcing the use of a central data repository would have ensured that project artifacts were easily and readily accessible for governance board reviews and general oversight.

3. **No Cumulative Cost and Schedule Documentation**

ITS did not maintain cumulative cost and schedule data as this was separately managed by each SU with the assistance of ITS R&D managers. Typically, system implementations (whether for a COTS product or for an in-house developed system) will involve a collaborative effort between: (1) the product vendor, (2) technical support personnel at the SUs and (3) technical/project support personnel from ITS. These three costs are tracked separately, oftentimes recorded in the division's operating expenses and not associated with the appropriate investment. Consequently, this impacts management's ability to monitor programs and projects effectively. We made requests to project oversight officials for the total cost, scheduled milestones, and schedule overruns for some IT projects in our samples, but ITS R&D managers were unable to provide the information and indicated that the requested documentation existed at the respective

SUs. Project management did not maintain cumulative life cycle development cost as ITS personnel costs for support personnel was not tracked.

This data would have allowed the CIO to identify, analyze, and monitor project costs and schedule overruns on LOC's IT projects. For example, certain IT enhancement projects have been in existence since 2009 and have not been completed. However, it was not obvious from project documentation whether the delayed implementation was due to fund availability or budget overruns.

Federal Government Best Practice requires that the Chief Information Officer (CIO) monitor and evaluate the performance of IT projects and advise the head of the agency regarding whether to continue, modify, or terminate an investment. LOC currently cannot determine the operating effectiveness of this process as project costs are not exhaustively captured[7].

4. **No ITS/PMO Oversight - Ineffective Monitoring of LOC IT Projects:**

The ITS Project Management Life Cycle guide was not effectively communicated or consistently applied throughout the Library. Without a clearly defined mandate to enforce SDLC processes Library-wide, the PMO's PMLC/SDLC guides are considered ITS guidance and do not carry the weight of Library-wide policies and procedures. Therefore, we concluded that LOC had not developed an effective strategy to communicate IT project guidance, which resulted in inconsistent management, a lack of accountability, and ineffective stewardship over LOC's major IT projects.

Furthermore, the last SDLC plan was developed in 2006. Although minor changes to SDLC processes have occurred over the years, the PMO has embarked on formally updating the SDLC plan on its intranet website. The revised SDLC has been available via a series of web pages on the PMO website at http://www.loc.gov/staff/pmo/sdlc.html since early 2011 and has undergone continuous improvements.

GAO's *Standards for Internal Control in the Federal Government* (GAO-17-704G September 2014) states that policies, procedures, techniques, and mechanisms that enforce management's directives are control activities, which help ensure management's directives are carried out. In addition, information should be recorded and communicated to management and others within LOC that need it within a time frame that enables them to carry out their internal control and other responsibilities.

5. **Significant Milestone Deliverables in the Life Cycle (Library Services) were not Documented or Executed.**

The seven phase SDLC framework was the model ITS used to manage ITS-related projects throughout their life cycles. This framework is meant to enable senior leadership to evaluate and make critical funding decisions about continuing or discontinuing[8] major IT projects at major decision points referred to as milestones. Each milestone marks the end of a phase and a critical decision point where a Milestone Review briefing is

---

[7] *See Report on the Library's Certification and Accreditation Policies, Procedures and Operating Effectiveness (October 2014).*
[8] *Management can decide to discontinue a project if there are potential budget overruns or if they realize the IT investment might be obsolete by the time the project is complete.*

supposed to be conducted. Milestone Review briefings provide a basis for comprehensive management, progressive decision making, and authorization of funding for each phase of the IT SDLC framework. The content of the Milestone Review briefing depends on the completed milestone phase of the project. By monitoring and measuring progress on a regular basis at each milestone, project managers can identify variances and take appropriate corrective actions.

Library Service's System Management Information Network (SYMIN) II went through an exhaustive system modernization and received its Authorization to Operate (ATO) without evidence of ITSC oversight and approval, although this project met three of the criteria that make it mandatory for certain projects of this nature to have this level of monitoring: (1) its project cost was estimated at $1.8 Million; (2) the system was to be used by multiple SUs; and (3) had high visibility.

In addition, Voyager – Integrated Library Systems (ILS) had incomplete or missing documentation. The documentation was either: (1) not final, such as the service level agreements; (2) not signed by an approving official, such as the Concept of Operations or Project Charter; or (3) did not exist, such as implementation plans. Yet, in spite of the incomplete or missing artifacts, the internal SU control boards approved these projects to progress from one phase to the next.

GAO's *Information Technology Investment Management Framework, A Framework for Assessing and Improving Maturity* (March 2004) states that to make good IT investment decisions, an organization must be able to acquire pertinent information about each investment and store that information in a retrievable format for use in making future investment decisions. During this critical process, the organization identifies its IT assets and creates a comprehensive repository of investment information used to track the organization's IT resources and provide insights and trends about major IT costs and management drivers. Based on our testing, there was no evidence that LOC maintained a comprehensive repository of all its IT projects.

LCR 1600 establishes uniform policy and responsibilities for IRM in the Library. It provides the foundation for an overall approach to IRM throughout the Library whereby IRM is integrated with the Library's strategic plan and reinforces the Library's Management Agenda. The regulation addresses the key concepts that support IRM, EA, and ITIM. It empowers the Librarian as custodian of IT Policies and Assets: Section 5 (a):

> *"…The Librarian is responsible generally for oversight of the Library's IRM plan and for all final determinations regarding the Library's IRM policy and IT investments…"*

These conditions occurred because the Library never fully centralized its IT Investment Management functions regarding the SDLC process. ITS has appointed R&D managers to assist each SU in managing its IT Investment Portfolio, but these R&D managers do not handle all of that portfolio, especially as it relates to self-sponsored IT systems owned by divisions that do cost-recovery. Consequently, some systems under the direct management of the SUs may not be managed effectively and efficiently.

We could not determine the value of this portfolio managed outside of direct ITS oversight as this information could not be readily obtained leaving some amount of LOC's IT projects at risk. This lack of a centralized process increased the risks that IT projects could experience cost and

schedule overruns, which could ultimately lead to other costly, unproductive, or failed programs and projects.

Recommendations:

We recommend that the Office of the Librarian:

1. Issue a policy that communicates, Library-wide, the mandatory requirements of the Library's System Development Life Cycle process outlined in the existing ITS Project Management Life Cycle Guide to ensure consistent management of the Library's Information Technology projects. Establishing a policy to enforce existing mandatory guidance would better ensure consistent oversight and provide a standardized framework for managing the Library's Information Technology projects

2. Establish a centralized Library-wide Project Management Office to communicate and enforce the Library's Project Management Life Cycle/System Development Life Cycle methodology and to ensure the Library's major IT projects are effectively managed in a consistent manner across all service units. The central PMO should continuously monitor all SDLC projects and update all SDLC plans and instructions for Library-wide distribution.

3. Perform disciplined uniform performance and quality reviews (preferably by the Project Management Office) on all major SDLC projects in the Library.

4. Establish budget methodology to track project development costs and measure variances against approved costs.

5. Establish a central data repository with the Enterprise Architect and/or PMO to store all project artifacts, including cumulative cost and schedule data. In addition, periodically perform an internal and/or external inspection of the Library's Information Technology Projects and update the Enterprise Architect repository with the results of the inspection if necessary.

6. Centralize the assessment of the Library's IT portfolio with the PMO and prohibit the existing practice of SU IT investment self-assessments.

7. Revise LCR 1600 to clearly delineate ownership and stewardship of IT assets.

VI. MANAGEMENT'S RESPONSE

LIBRARY OF CONGRESS

OFFICE OF THE LIBRARIAN

MEMORANDUM

DATE February 10, 2015

TO Kurt W. Hyde, Inspector General

FROM David S. Mao, Deputy Librarian of Congress

SUBJECT Audit No. 2013-IT-105 – SDLC – Management Comments on Draft Report

Thank you for the opportunity to comment on the draft report for Audit No. 2013-IT-105, *Report on the Maturity of the Library's System Development Life Cycle Processes and Procedures.* Below please find management comments on the report's recommendations.

1. Issue a policy that communicates, Library-wide, the mandatory requirements of the Library's System Development Life Cycle (SDLC) process outlined in the existing ITS Project Management Life Cycle (PMLC) Guide to ensure consistent management of the Library's Information Technology projects.

    Management Comment: The Library agrees with this recommendation.

2. Establish a centralized Library-wide Project Management Office (PMO) to communicate and enforce the Library's PMLC/SDLC methodology and to ensure the Library's major IT projects are effectively managed in a consistent manner across all service units.

    Management Comment: The Library agrees that central oversight of IT projects is valuable. At this point, however, Library management does not agree that establishing a separate PMO is the most efficient approach. The Library will assess whether to assign this function to the ITSC (or another existing body) or to establish a new office.

3. Perform disciplined uniform performance and quality reviews (preferably by the PMO) on all major SDLC projects in the Library.

    Management Comment: The Library agrees with this recommendation, and will determine whether to perform these reviews internally or outsource this function to an independent validation and verification contractor.

Page 1 of 2

4.   Establish budget methodology to track project development costs and measure variances against approved costs.

> *Management Comment:* The Library agrees with this recommendation. This would be developed in conjunction with any work currently underway with the OCFO .

5.   Establish a central data repository with the Enterprise Architect and/or PMO to store all project artifacts, including cumulative cost and schedule data. In addition, periodically perform an internal and/or external inspection of the Library's Information Technology Projects and update the Enterprise Architect repository with the results of the inspection if necessary.

> *Management Comment:* The Library agrees with this recommendation and will assess whether the enterprise architect, the ITSC secretariat, or another body would best serve as the appropriate repository for IT project artifacts.

6.   Centralize the assessment of the Library's IT portfolio with the PMO and prohibit the existing practice of service unit IT investment self-assessments.

> *Management Comment:* The Library agrees that centralizing the assessment process will facilitate accountability. The Library will evaluate whether to assign this function to the ITSC (or another existing body) or whether to establish a new office.

7.   Revise LCR 1600 to clearly delineate ownership and stewardship of IT assets.

> *Management Comment:* The Library agrees that LCR 1600 should clearly delineate the roles of "ownership" and "stewardship" of IT assets, and should establish the process for recording who performs each role for each asset.

Please let me know if you have any questions or would like to discuss this report.

LIBRARY OF CONGRESS
SYSTEM DEVELOPMENT LIFE CYCLE EVALUATION

LIST OF ACRONYMS USED

ARB	Architecture Review Board
ATO	Authorization to Operate
CLA	CliftonLarsonAllen LLP
CMMI	Capability Maturity Model Integration
COTS	Commercial Off the Shelf
EA	Enterprise Architecture
FAM	Financial Audit Manual
FISCAM	Federal Information System Controls Audit Manual
GAO	U.S. Government Accountability Office
ILS	Integrated Library System
IRM	Information Resource Management
ISO	International Organization of Standardization
IT	Information Technology
ITIM	Information Technology Investment Management
ITS	Information Technology Service
ITSC	Information Technology Steering Committee
LCR	Library of Congress Regulation
LOC	Library of Congress
LS	Library Services
OIG	Office of the Inspector General
OSI	Office of Strategic Initiatives
PCIE	President's Council on Integrity and Efficiency
PMLC	Project Management Life Cycle
R&D	Research and Development
SDLC	System Development Life Cycle
SEI	Software Engineering Institute
SU	Service Unit (of the Library of Congress)
SYMIN	System Management Information Network